UNCLASSIFIED

Defense Technical Information Center Compilation Part Notice

ADP010879

TITLE: Design Aspects in a Public Key Infrastructure for Network Applications Security

DISTRIBUTION: Approved for public release, distribution unlimited

This paper is part of the following report:

TITLE: New Information Processing Techniques for Military Systems [les Nouvelles techniques de traitement de l'information pour les systemes militaires]

To order the complete compilation report, use: ADA391919

The component part is provided here to allow users access to individually authored sections of proceedings, annals, symposia, ect. However, the component should be considered within the context of the overall compilation report and not as a stand-alone technical report.

The following component part numbers comprise the compilation report:
ADP010865 thru ADP010894

UNCLASSIFIED

Design Aspects in a Public Key Infrastructure for Network Applications Security

(August 2000)

Prof. Dr. VICTOR-VALERIU PATRICIU
Cdor.Prof. Dr. AUREL SERB
Computer Engineering Department,
Military Technical Academy,
Bd. G.Cosbuc nr.81-83, sect.4, Bucharest,
Romania

Abstract: Computer security is a vitally important consideration in modern systems. Typically, the military and banking areas have had detailed security systems. This paper will concentrate on an interesting area of software security based on public key cryptographic technology. The Public Key system makes it possible for two parties to communicate securely without either having to know or trust the other party. This is possible because a third party that both the other parties trust identifies them, and certifies that their keys are genuine. This third party is called the Certification Authority, or CA. CA guarantees that they are who they claim to be. The CA does this by registering each user's identification information, and issuing them with a set of Private keys and a set of Public Key Certificates. A worldwide Public Key Infrastructure (PKI) that supports international, government, and state policies/regulations will not be available in the near future. In the meantime, organizations and corporations can utilize this security technology to satisfy current business needs. Many organizations are choosing to manage their own Certificate Authority (CA) instead of outsourcing this function to a third party (i.e., Verisign, Thawte, GTE CyberTrust, GlobalSign). Our paper try to analyse the main design issues for a Public Key Infrastructure (PKI), needed to secure the most important network applications: Web access authentication and server-client communication confidentiality, VPN over Internet implementation, secure (signed) document and e-mail interchange.

1. INFORMATION SECURITY

Information security is now the major issue facing today's electronic society. For instance, e-mail now carries not only memos and notes, but also orders, contracts and sensitive information. The Web is being used not only for publishing corporate brochures but also for placing some organization's sensitive information, needed in the decision process. Virtual private networks (VPNs) are extending organization networks onto the Internet for remote network access. Extranets turn the Internet into dedicated, secure links between organization (military) partners for information exchange. Moreover, e-commerce is a competitive imperative for business worldwide; it is the fastest growingchannel for marketing, selling, documenting and distributing products and services, most of them needed for military purposes.

Why do we need information security? Although all nations have their own classified estimations of the threats their computer systems face, the following quotes from unclassified sources provide a strong indication of the magnitude of that threat:

- "More than 120 countries already have or are developing computer attack capabilities." Defence Science Board;
- "It is estimated that the DoD is attacked about 250,000 times a year ..." Defence Information Systems Agency (DISA);
- "Computer attacks have also become easier to carry out due to the proliferation of readily-available hacker information, tools, and techniques on the Internet." General Accounting Office (GAO);
- "Any marginally computer literate individual can use the Internet itself to quickly obtain basic information on the tools and techniques needed to become a computer hacker" GAO.

Given the severity of the threat, it is clear that unprotected communication and information systems are at risk. If they are not protected, organizations in **Romanian Armed Forces (RAF)** will experience (1) exposure of classified information to unauthorized persons, (2) destruction of critical data or, just as problematic, loss of confidence in the correctness of the data and (3) a potential loss of control over its forces. Finally, the performance of inadequately protected CIS could be degraded or reduced to zero at critical points in time by adversaries.

Ensuring adequate information security for military CIS systems require the development and evolution of an effective Information Security (INFOSEC) architecture that is based on a thorough understanding of the threat, system vulnerabilities and availability of counter-measures for protecting his own CIS. Another principal guidelines used in creating integrated security architecture are the need to ensure adequate protection of NATO classified information that is shared with Romania. As an alliance of independent sovereign states, NATO depends on the cooperation of its members to ensure adequate levels of security for shared information.

Paper presented at the RTO IST Symposium on "New Information Processing Techniques for Military Systems", held in Istanbul, Turkey, 9-11 October 2000, and published in RTO MP-049.

2. SECURITY ARCHITECTURE

When developing architecture, it is important to understand the underlying security principles, the basic security services and associated mechanisms and specific building blocks that can be used as the basis for creating the architecture. *Absolute total security of all military CIS resources simply cannot be afforded.* A corollary of this principle is that *total multi-level security (MLS) solutions are not realistic*–no one can afford to put a trusted workstation on every desktop. This fact is driven by the excessive cost and time required to produce products which have the necessary level of trust to be judged multi-level secure. All security system designers, managers and decision-makers need to be prepared to deal with residual risk. In other words, the use of operational procedures, audit reduction and monitoring, and other techniques will be needed to handle those risks that cannot be totally overcome by the technical design of CIS security features.

Since each and every desktop, server and network cannot be protected in an absolute sense, a better alternative is to provide strong protection at the enclave level. In its simplest terms this means providing the strongest security at the boundaries of an enclave where it is connected to less trusted or untrusted networks. Internal to an enclave less stringent technical security measures would be used, backed up by operational procedures and other techniques.

Highly interconnected networks and systems are a fact of life. The World Wide Web and related technologies are driving a trend toward new ways of accessing information, new information services and distributed processing that the military cannot afford to ignore technically or operationally. However, with all of these new capabilities come increased risks via network interconnections. In this environment, if a hostile agent can gain access to and subvert one workstation or server on a network that is "trusted," it can use that access to penetrate the remainder of the systems. Therefore, it is important that the "weakest link" be protected.

The level of protection afforded a system should be based on the value of the information that it contains, or the function that the system performs. In most military systems the value is a direct function of the classification of the data on that system and its military mission category.

There are a number of security risks. To reduce these risks, some **security services** have evolved over time. Table 1 lists these services along with the **security mechanisms** that can be used to provide the service.

Table 1. Security Services and Mechanisms

Service	Mechanism
Confidentiality	Encryption (link, bulk, E3) Access control (MAC/DAC)
Integrity	Digital signature Access control (MAC/DAC)
Availability *(Denial of Service)*	Encryption (link, bulk, E3) Digital signature Access control (MAC/DAC)
Authentication	Encryption (digital signature)
Non-repudiation	Encryption (digital signature)

- **Confidentiality** services ensure that the contents of the message have not been disclosed to third parties and data is not accessed, seen or otherwise available to unauthorized users whether it stored on a workstation or server or in transit over a network. Confidentiality requirements are enforced by using access control mechanisms on computers and by encrypting data while it is in transit over a network and sometimes while it is stored on disk. There are many types of encryption including link, bulk and end-to-end encryption (E3).
- **Integrity** services proof that the message contents have not been altered or destroyed, deliberately or accidentally, by an unauthorized action. Mechanisms used to protect the integrity of data include message hashing, encryption and access controls. Message hashing is a technique that creates a "checksum" based on a "one-way" function and attaches it to the data. Digital signatures are a special encryption technique; the encryption process does not encrypt the "text," but instead encrypts the message hash and other data designed to prevent replay and other types of attacks. Access controls limit access to data to authorized personnel that prevents system users who aren't authorized access to that data from altering the data.
- **Availability** is focused on ensuring that a particular resource is accessible and useable upon demand by authorized personnel, i.e., that they are not denied access and use by an adversary. Again, encryption is used to prevent sophisticated attacks against networks and computer systems over communication links while access controls are used to prevent unauthorized personnel from shutting them down.
- **Authentication** is a mechanism by which a user proves he is who he says he is. In computer systems and networks, some mechanism is needed to ensure that the identification supplied is in fact the real identity of the individual. Historically, this has been done with simple passwords but that has proven to be ineffective against today's hackers. There are many techniques being used in modern identification and authentication systems but all of the strong ones depend on encryption and many depend on digital signatures.

- **Non-repudiation** is a service that prevents entities involved in a communication exchange from denying that they participated in that exchange. For example, non-repudiation can be used to prove that a certain user originated a message and that another user received that message. Again, digital signatures provide a strong technical solution for this requirement.

Development of a **top-level security architecture** is easier if one uses generic components to create it. These components fall into *two main **generic categories***:

- ***Communication security (COMSEC)***, based on the use of encryption (both symmetric and asymmetric) and associated security protocols and key management, protects data in transit;
- ***Computer security (COMPUSEC)***, refers security techniques embedded in computer systems that enable those systems to be "trusted".

3. NEED FOR PKI

Having established the need for security, looked at how NATO views security and reviewed some basics of security architectures, it is time to consider the *technologies that are available to put together a meaningful architecture and system design.* Computer security technology involves understanding what it means to "trust" a system and how one can achieve the requisite level of trust. The "*Common Criteria*" provides a framework for achieving trust. *Public key cryptography* is a relatively new technology that provides a number of important security capabilities that can be used by security architects. *Protect, detect and react tools* are being driven by the marketplace and the ever expanding use of the global Internet for commerce. These tools are extremely useful in countering many of the security threats that are a natural outgrowth of the "openness" of Internet technologies and the impossibility of writing totally correct software. *Firewalls and Guards* are two examples of technology solutions designed to provide a *perimeter defence.*

The new approach in modern cryptography, based on public keys, enables the provision of a *digital signature* capability, non-repudiation, strong identification and authentication, secure key exchange and ad hoc secure communications. In order to provide these services, a **Public Key Infrastructure (PKI)** is required. This infrastructure depends on certificate authorities to create and sign certificates for all of the users of the public key system. These certificates, which are signed by the certificate authority, provide the public keys of users and generally are entered into a public directory so that anyone can access them. In general, *public key cryptography is a computationally intensive technology and is not suitable for the encryption of files, long messages*, etc. It is, however, *suitable for digital signature and key exchange.* Symmetric keys are suitable for encrypting data but not for digital signature or ad hoc exchange of keys. Consequently, in the vast majority of applications a combination of public key and symmetric key cryptography is used to best advantage. More western countries, U.S. and NATO are in the process of selecting and fielding PKI systems at this time.

PKI as defined herein refers to the framework and *services that provide the following*:

- generation, production, distribution, control, revocation, archive and tracking of public key certificates,
- management of keys,
- support to applications providing confidentiality and authentication of network transactions,
- data integrity, and
- non repudiation.

The organizational (military) PKI shall provide an integrated public key infrastructure that supports a broad range of commercially based security-enabled applications and provides secure interoperability with the military and commercial partners while minimizing overhead and impact to operations. It is the objective of the PKI to provide *certification services that have the following characteristics*:

- support multiple applications and products;
- provide secure interoperability throughout the military organizations and with its partners such as government agencies, industry and academia;
- standards based;
- uses commercial PKI products to minimize the investment and the manpower to manage the PKI;
- support digital signature and key exchange applications;
- support key recovery;
- employs centralized certificate management and decentralized registration;
- support Federal Information Processing Standards-FIPS compliance requirements.

4. PKI COMPONENTS

In a PKI, there are several different entities or components. These components may be implemented separately, but are commonly integrated and delivered through what are called **Certificate Servers**.

1. **Certificate Authority (CA)** is the most fundamental component that will authorize and create digital certificates. A certificate authority (CA) server issues, manages, and revokes certificates. The CA's certificate (i.e., public key) is well known and trusted by all the participating end entities. The CA can delegate its authority to a subordinate authority by issuing a CA certificate, creating a certificate hierarchy. This is done for administration (e.g., different issuance policies) and performance reasons (e.g., single point of failure and network congestion). The ordered sequence of certificates from the last branch to the root is called a certificate chain. Each certificate contains the name of that certification's issuer (i.e., this is the subject name of the next certificate in the chain). A self-signed certificate means that the signer's public key corresponds to it's

private key (i.e., the X.509v3 issuer and subject lines are identical).

2. The second core component of a PKI is the **Registration Authority (RA)**, which provides the mechanism and interface for submitting users' public keys and identifying information in a uniform manner, in preparation for signing by the CA.
3. The third component is a **Repository (Directory Server)** in which certificates and certificate revocation lists are stored in a secure manner for later retrieval by systems and users. *Lightweight Directory Access Protocol (LDAP)* was originally designed to make it possible for applications running on a wide array of platforms to access X.500 directories. LDAP is defined by RFCs 1777 and 1778 as an on-the-wire bit protocol (similar to HTTP) that runs over TCP/IP. It creates a standard way for applications to request and manage directory information (i.e., no proprietary ownership, or control of the directory protocol). The directory entries are arranged in a hierarchical treelike structure that reflects political, geographic, and/or corporation boundaries.
4. **PKI Applications** are those use public-key technology. In most cases, the application would provide underlying cryptographic functions (e.g., public/private key generation, digital signature, and encryption) and certificate management. Certificate management functions include creating certificate requests, revocations, and the secure storage of a private key(s). Examples of PKI applications include Netscape's SSL 3.0 browser/server, Deming's Secure Messenger, and GlobeSet's Secure Electronic Transaction (SET) Wallet, Microsoft Outlook mail system.

5. PKI COMPONENT SECURITY REQUIREMENTS

PKI components each share a set of security requirements (i.e., baseline) with each other. The baseline corporate PKI security requirements are as follows:

- Reliable software (i.e., a comfortable level of assurance that security software is implementing the cryptographic controls properly).
- Secure/trusted communications between components (e.g., IPSec, SSL 3.0).
- PKI specific security policies that are derived from the existing set of corporate security policies.

Most PKI software/hardware is built upon cryptographic toolkits (e.g., RSA's B-Safe). The application that calls the lower level functions in the toolkit is still prone to human errors. Every other month Microsoft and Netscape release bug fixes for their Internet product sets. If the browser wars continue, there will be shorter quality assurance cycles to meet the current time to market constraints, hence produce a lower quality of software. PKI components require authenticated and private communication among each other. This prevents active or passive threats (e.g., eavesdropping, spoofing) from occurring. Most current implementation of PKI components supports SSL 3.0. Each component has a security criterion it must meet to be part of a PKI. This criterion is based on the level of protection necessary to perform the business objectives within the acceptable level of risk. The security mechanisms used to meet this criterion usually falls into physical, platform, network, and application categories. These categories are not all included in the PKI applications and have to be supplemented. Examples of these are network firewalls, disabling NFS exports, authenticated naming services, and tight administrator controls (e.g., root user).

Certificate Authority

The certificate authority security requirements are:

- Certificate generation, issuance, inquiries, revocation, renewal, and storage policies.
- Certification Practice Statement (CPS).
- Certificate attributes or extension policies.
- Certificate administration, audit journal, and data recovery/life-cycle support.
- Secure storage of private keys.
- Cross certification agreements.

The applicability and/or usage of the certificate the CA manages are defined in the **Certificate Policy (CP).** A security policy must exist for each CA function (e.g., generation, issuance, revocation list latency, etc.). These policies are the foundation upon which all the CA security related activities are based on **Certification Practice Statement (CPS)** is a detailed statement by the CA as to its certificate management practices. The certificate end entities and subscribers need to be well aware of these practices before trusting the CA. The CPS also allows the CA to indemnify itself to protect its relationships.

One of the major improvements to version 3 of X.509 is the ability to allow flexible extensions to the certificate structure. These extensions include additional key and policy information, user and CA attributes, and certification path constraints. The CA must document, by way of a policy, the certificate attributes and extensions it supports. In addition, to allow interoperability outside the corporation, one must register the extension object identifiers (OID) with the American National Standards Institute (ANSI).

The CA must maintain an audit journal of all key management operations it performs. All certificate management functions must be audited (e.g., issuance, revocation, etc.) in case of a dispute. In conjunction with this auditing function, a data recovery and certificate life cycle plan must also exist. The CA administrator interface must enforce the least privilege principal for all administrator actions.

The certificate authority must provide for the adequate protection of the private key that it uses to sign certificates. The machine that the CA runs on must be protected from network and physical intrusions. Optionally, the CA's private key used to sign certificates can be stored in a tamperproof hardware module (e.g., meets FIPS PUB 140-1 level 3).

Cross-certification certificates are issued by CAs to form a non-hierarchical trust path. Two certificates are

necessary for a mutual trust relationship (i.e., forward, and reverse directions). These certificates have to be supported by an agreement between the CAs. A cross-certification agreement details the obligation of liability between partners if a certificate turns out to be false or misleading.

Directory Server

The directory server security requirements are as follows:

- Supports network authentication through IP address/DNS name, and user authentication through LDAP user name and password, or a X.509 version 3 public-key certificate.
- Controls the users' ability to perform read, write, search, or compare operations down to the attribute level.
- Provides message privacy (SSL) and message integrity for all communications.

The directory server contains corporate and user personal attribute information. Access to this information must be controlled at the most granular level possible. Directory administrators must be able to restrict particular users from performing specific directory operations (e.g., read, write, search, and compare). Authentication must support conventional username/passwords and/or certificates. Additional filtering should be provided using IP address/DNS name. Network access to the directory server must be able to be protected between all PKI components.

PKI Clients

All PKI clients, at a minimum, must be able to generate digital signatures and manage certificates. PKI client requirements are as follows:

- Generate a public/private key pair.
- Create a certificate request (PKCS#10).
- Display certificate.
- Verify certificate.
- Delete certificate.
- Enable or disable multiple certificates.
- Request a certificate revocation.
- Secure storage of certificates (e.g., password, and hardware).
- Secure exporting certificates (e.g., PKCS #12).
- Select algorithm, key strength, and password controls.
- Configure security options (e.g., sign/encrypt whenever possible).

The process begins with a PKI client generating a public/private key pair locally. The software used to generate the public/private key pair must use a non-deterministic algorithm. Once the key pair is generated, the public portion needs to be bound inside a certificate structure. The PKI client must then generate a certificate request adhering to the PKCS#10 syntax and submit that information to a CA. Once the CA fulfils the request, the message response sent back to the client is in PKCS#7 syntax (i.e., signed envelope). All network traffic is kept private between the client and the CA.

The PKI client must have the ability to manage multiple certificates. This includes viewing the certificate structure (e.g., subject, issuer, serial number, fingerprint, and validity dates); deleting it, if necessary; choosing (i.e., enabling) what certificate to use or query the user; or requesting the CA to revoke it.

A large portion of public cryptography is based on the protection of the private key. The PKI client must protect their private key commensurate with the risk associated with the loss of all the transactions it processes. This will require encrypted storage of the key using an application authentication challenge (e.g., organization compliant password), or hardware token or smart card, and the user physically protecting their desktop (e.g., password protected screen saver).

Due to the infancy of this technology, certificates are bound to the PKI client application software and hence the host that the software resides on. An emerging public key cryptographic standard (PKCS) called personal information exchange syntax standard (i.e., PKCS #12) details the transfer syntax for personal identity information. This includes private keys, certificates, miscellaneous secrets, and extensions. This will allow PKI clients to import and export personal identity information across multiple platforms and applications. The most secure method includes a privacy and integrity mode that requires the source and destination platforms to have trusted public/private key pairs available for digital signatures and encryption. The least secure method protects personal identity information with encryption based on a password.

6. CERTIFICATES AND REVOCATION LISTS

The certificate tipical forma is ITU's **X.509v3**. PKI clients support their own **certificate types** (e.g., mail, browser). Before a certificate can be requested from a CA it is necessary to have access to the CA's certificate in the PKI client. Typical certificates are the following:

- *Certificate Signer/Provider*-These external institutions provide an outsourced CA function. They are usually preloaded into the PKI client application (e.g., VeriSign Class 2 Primary CA, GTE CyberTrust).
- *Sites/Hosts*-This is a list of sites/hosts that the PKI client has stored locally. The importing process for this varies depending on the application vendor. Netscape's browsers allow importing site/host certificates from non-certificate signers/providers over SSL. Microsoft requires a more stringent trust model that most CA vendors use insecurely.
- *Code Signer/Provider*-The code signer/provider certificate allows Java applets or ActiveX scripts to verify message authentication (i.e., data integrity) before they are executed.
- *Cross –Certification*- A cross-certification certificate defines a one-way trust path between CAs.
- *Personal*-Personal certificates are used to identify one's self to other PKI clients that require authentication and/or privacy.

- *File-* A file certificate is used to encrypt or sign local files. This certificate is only shared with a key recovery server.
- *Key Recovery-* A certificate used between the key recover servers.
- *PKCS #12-* PKCS#12 optionally requires a pair of certificates; one for encryption and the other for signing each host that requires the secure transfer of private key information.

7. ARCHITECTURE REQUIREMENTS FOR CA

The target PKI employs centralized certificate management and decentralized registration shown in Figure 1 and uses common processes and components to minimize the investment as well as the manpower required to manage and operate the PKI.

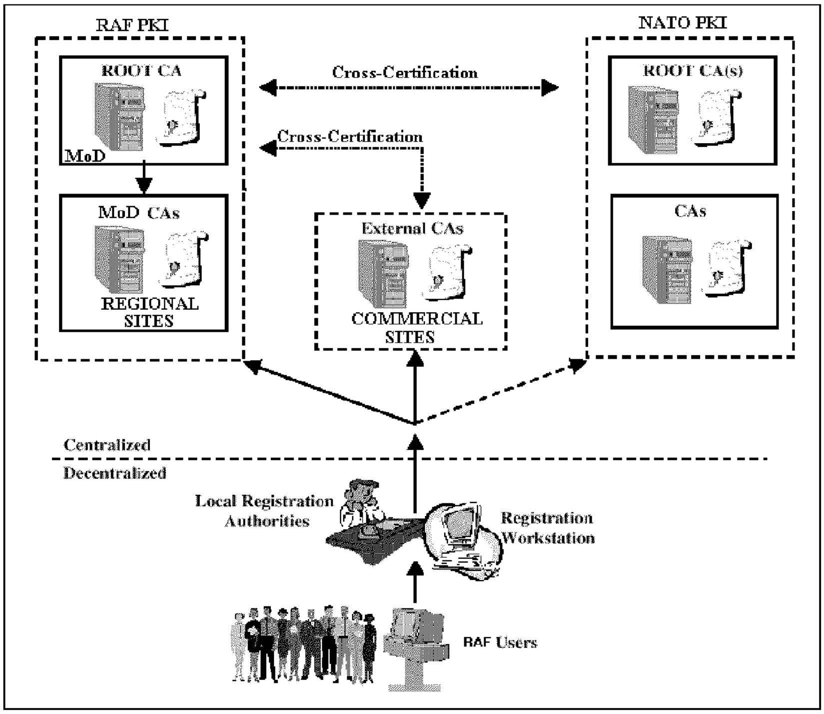

Figure 1 PKI CA Architecture

The centralized portion of the certificate management process shown in Figure 1 is comprised of a combination of military owned and operated components. The Defense Minister will manage and operate its Root CA s. The Root CAs is responsible for managing subordinate CAs and External CAs (ECAs) and cross certifying with other domains for interoperability. The Root CA s will be operated as offline devices with maximum physical personnel and procedural security protections. A standards based certificate request format (e g PKCS #10 or RFC 2511) will be used to interface with the Root CA s and register subordinate CAs into the system in a trusted out of band process.

Based on current technology limitations it is envisioned that it will require separate CAs on each of its networks, similar to the current implementations today where identical PKIs are replicated on each network. The CAs that support classified mission critical command and control applications will be under the direct control of the Root CA s and will be owned and operated by the Defense Ministry. They are networked devices supporting a standards based secure interface for the Local RAs for user registration. They will be operated with the technical physical personnel and procedural security protections as defined in the military regulations. It is expected there will only be a small number of CAs located at several regional sites. The target PKI plans to eventually achieve secure interoperability with non-military entities through a process called "direct cross certification" which establishes a policy and process for recognizing third party CAs.

The registration function is decentralized in the target PKI with **Registration Authorities (RA**s) responsible for user identification. The military Services and Agencies will manage registration. It depicts a common workstation and web based application with hardware token. A common registration workstation with unified ordering and delivery software will be based on commercial standards and technologies. The target envisions a common set of processes and tools so that the only differences between assurance levels from the RAs' and users' perspective are the user identification procedures and tokens protecting the keys. This will allow users to register with the appropriate CA server

through a single RA. This single registration workstation should be able to transparently register users into CAs commercial certificate service providers or other external CAs as needed.

End users commonly referred to, as end entities can be a person a machine such as a router or a process running on a computer such as a firewall. The target PKI will need to provide support for all end entities including non-human Registration of end entities will use a common registration application to securely register with the infrastructure. During registration the user's token will generate a digital signature key pair public and private key and send the public key to the CA. Once the CA returns the certificate, the user can then load the certificate onto the token (smartcard, Universal Serial bus USb device or personal computer PC card).

User registration process employs pre-registration and direct delivery of the certificate and key information to the end user or equipment. As an example one potential implementation is the following:

1. The RA making use of this common web based registration application securely authenticates e g SSL to the appropriate CA servers via a common KMI management front end and registers the user s.
2. Next the RA identifies the user as required by the policy and provides the necessary information for the user to authenticate to the CA server.
3. The CP specifies the authentication requirements process for the various assurance levels. After receiving the authentication information the user can use a common registration application to securely connect to the appropriate CA server and request a certificate.
4. During registration the user's token or software application will generate a digital signature key pair public and private key and send the public key to the CA server.
5. The CA server processes the request verifies possession of the private key generates the certificate posts it to the directory system and returns the certificate to the user.
6. The user can then load the certificate onto the token (e. g. smartcard, Universal Serial Bus USB device, or personal computer PC card). This token certificate can be used in a variety of applications allowing a single registration to support multiple applications. Once the user has a digital signature certificate he she can use that certificate to request additional certificates such as encryption or attribute certificates at the same assurance level.

8. CASE STUDY: RSA KEON CERTIFICATE SERVER

This case study is an implementation of a PKI using RSA Security suite of products, particularly *RSA Keon Certification Server (KCS)*. The PKI clients were Netscape's Navigator 4.1 and Microsoft Internet Explorer 5.0 and Outlook Express. The outcome of the effort fields an organization level PKI, including client authentication and secure e-mail (S/MIME) using a self-signed root. This solution addresses the security problems of an organization and prepares the steps necessary for creating a *PKI pilot centre*.

RSA Keon is a family of products of RSA Data Security S.A., which can be applied to deliver organization level security through the application of public/private key-based cryptography. The RSA Keon product family expands beyond this definition to include an RSA Keon Security Server, RSA Keon Desktop, RSA Keon Agents. The components that provide for the creation and management of public/private keys and the associated digital certificates make up a PKI. Across vendors, there may be some variation in the components that make up a PKI, but the most common set of components is:

- A *Certificate Authority* (CA), an entity which issues certificates;
- A *repository* for public key certificates and *Certificate Revocation Lists* (CRLs) usually based on a Lightweight Directory Access Protocol (LDAP)-enabled directory service;
- A *management function*, typically implemented via a management console (RA).

RSA Keon Certificate Server integrates the functions of a CA, RA and Repository into a single system, as shown in Figure 2.

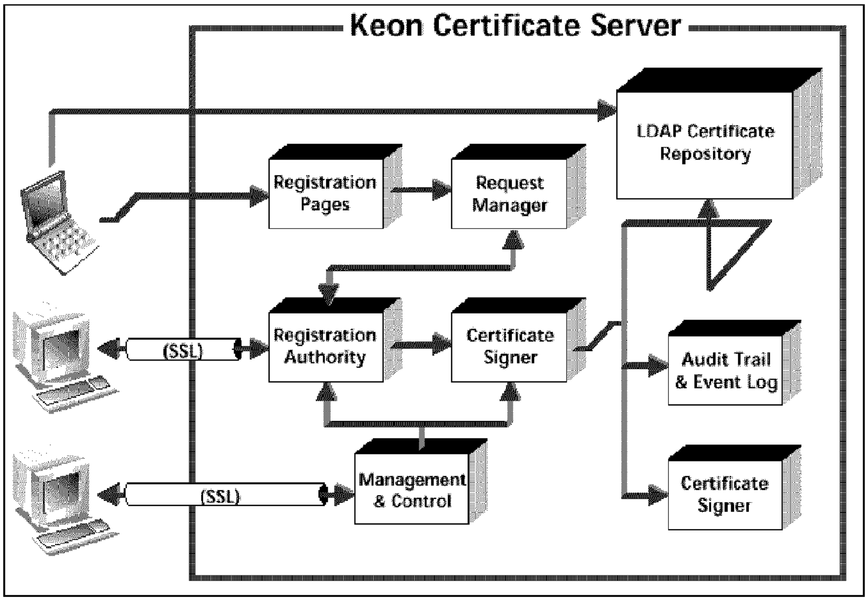

Figure 2 RSA Keon Certificate Server Architecture

The Keon Certificate Server is based strictly on open-standards. Organizations can rest assured that they are not tied to a vendor's proprietary solution, which will only work with other products from that same vendor.

Instead, companies using the Keon Certificate Server can deliver certificates that will interoperate with PKI solutions from any vendor that follows the popular PKI standards in existence, such as LDAP, PKCS #7, PKCS #10, X.509v3, and PKIXv1. RSA Keon Certificate Server was designed to inter-operate with standard, off-the-shelf, PKI ready applications from **Netscape** and **Microsoft**. At the RSA Keon Certificate Server, certificates and CRLs can be published to the bundled Netscape LDAP directory or to other LDAP compliant directories. As a result the RSA Keon Certificate Server can be replaced with other Certificate Servers that implement standard X.509 v 3 certificates, such as **VeriSign OnSite**.

Secure administration of KCS is handled through simple Web interfaces protected by digital certificates and SSL. The certificate delivery and granting process can be automated so that no administrator intervention is required. In addition, a full suite of complementary tools is available for integrating existing and new applications into the PKI. The BSAFE line of software development kits (SDKs) from RSA Security can be used to PKI-enable applications.

RSA Keon Certificate Server, acting as a trusted entity known as a **Certificate Authority (CA),** include two entities:

-**System Administrator**- which designates Certificate Administrators and configure components of system- *Signers*, *Signers Hierarchies*, *Jurisdictions*, *Directory* and

-**Certificate Administrators**-, which manages certificates for subscribers.

Figure 3 explains the process of certificate administration in a Keon Certificate Server context. The Keon CA:

- control over **who has access to your organization's information** on Intranet /Extranet,
- control over **access to sensitive data,**
- establish & publish the **Statement of Practice** document,
- control over **who signs certificates** by specifying signers and jurisdictions,
- control over **certificate granting,**
- **issues** and **manage** certificates,
- **digitally signs** subscriber's certificate,
- **made up** of entities within your organization or within an external source, a **trusted third party** (eg.**Verisign**).

In this context, **Certificate Server** & **System Administrator** act as CA and **Certificate Administrator** acts as agent of CA. RSA Keon Certificate Server (KCS) enables **policies** and **practices** of:

-certification,
-certificate revocation,
-certificate management,
-additional certificate activities.

KCS is accessed through a 2 **Web browser**:

-**CA Center** for System Administrator,
-**Control Center** for Certificate Administrator.

KCS generates and distributes **3 distinct types of certificates**:

-**Personal Certificates**

>Netscape & Microsoft Personal
>CSR (Certificate Signing Request) Personal, for applications that produce certificate requests.

-**Secure Server Certificates** (Web server)

-**Internet Protocol Security (IPSec) Certificates** (between routers- IP layer).

Using the concept of **jurisdiction**, KCS divides Subscriber population into groups. Each Jurisdiction is managed by a different Certificate Administrator (e.g. Engineering Jurisdiction, Finance Jurisdiction, IT Jurisdiction) and simplifies the certificate management. Each Jurisdiction may be configured to use only specified certificate types. Several Signers may be allocated to a Jurisdiction but only one Signer can be allocated per certificate type.

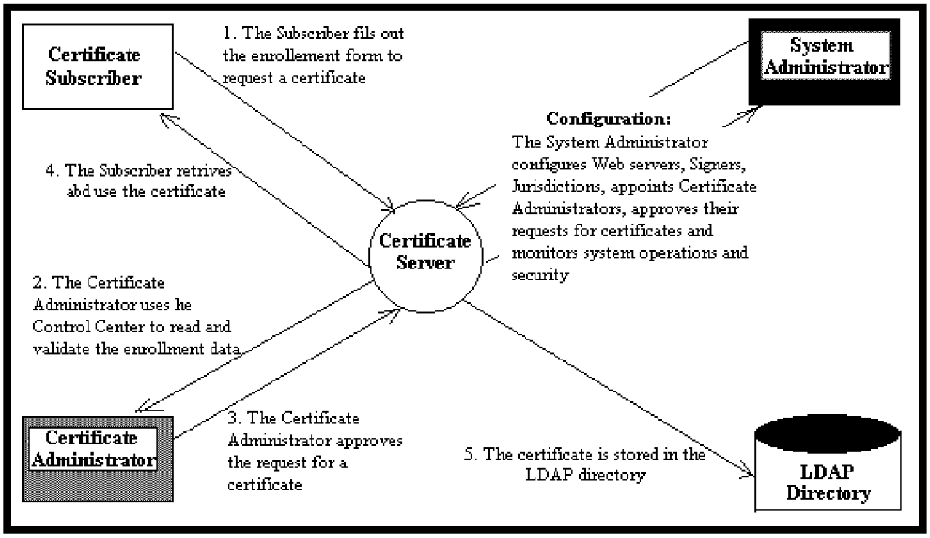

Figure 3 Certificate Management Process

Another notion used by KCS is **signer**: a cryptographic key that the signing software in KCS uses to sign a certificate. Using the Signer, KCS digitally signs the information that a subscriber entered in the *Certificate Enrollment Form*. The result is a certificate. Each Signer has a unique name that appears in each certificate. Figures 4 illustrate the signer's hierarchy.

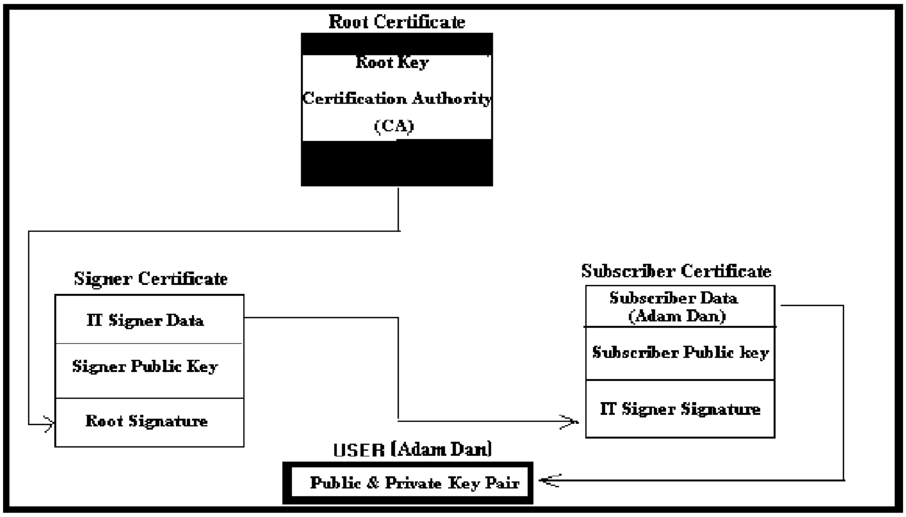

Figure 4 Hierarchies of signers

System Administrator has the following *responsibilities*: installing & configuring, managing signers, managing jurisdictions, configuring, Directory Server interface, and scheduling the creation of CRL. His *day to day tasks* are: appointing qualified Certificate Administrators, auditing & monitoring system security, managing System Administrator certificates, providing support for Certificate Administrators.

Certificate Administrator has the following *responsibilities*: configuring the enrollment pages, customizing the Subscriber agreement. His *day to day tasks* are: validating the identities of applicants, approving or rejecting Certificate requests, assigning requests to other Administrators, revoking certificates, providing support for Certificate Subscribers.

There are many **applications that require a Certificate Server in order to function**. We will examine three of them: Web access authentication and server-client communication confidentiality, secure (signed) document and e-mail, and virtual private networks (VPN).

1. **Secure E-mail and Messaging**

Many organizations rely on e-mail to distribute sensitive information. Unsecured e-mail can be intercepted, read and modified while in transit from sender to receiver, without the knowledge of either party. Worse still, today's e-mail systems make it very easy for attackers to create phone messages, create false orders, and disrupt business operations. An organization PKI based on digital certificates from a Certificate Server is the solution to these problems. In secure e-mail systems, a Certificate Server supplies digital certificates that plug in to existing mail clients including Microsoft Outlook, Netscape Messenger, and Eudora. These clients are all able to leverage the power of digital certificates and the S/MIME secure messaging standard out-of-the- box or through plug-ins. In addition to e-mail, message-based applications such as EDI and electronic billing are useful because they provide asynchronous delivery of documents. Security for these other applications can be accomplished using S/MIME technology in combination with a Certificate Server.

2. **Web Applications**

The Web plays a huge role in organization today. However, security continues to be a problem. In the case of Intranets, physical security measures and firewalls are sufficient to keep external parties from accessing sensitive internal Web pages. However, a means needs to exist to keep sensitive information from other employees within the organization firewall. The technology that solves these problems and enables secure Web is the Secure Sockets Layer (SSL) protocol. The protocol allows Web servers and Web clients to securely share information across networks, both inside and outside of the firewall. Any Web application or server that contains an SSL engine for secures connections only needs a digital certificate from a trusted Certificate Server to enables Web security. In fact, the ability to perform secure Web access through SSL already exists in Web clients such as Netscape Navigator and Microsoft Internet Explorer. Web servers such as Netscape Enterprise Server and Microsoft IIS are already SSL-capable. In virtually all organizations today, the only component missing from activating secure Web access is digital certificates from a Certificate Server. Using a Certificate Server, organizations can issue digital certificates to employees, Web servers, customers, and partners that enable access to Web resources from inside and outside the firewall.

3. **Virtual Private Networks (VPNs)**

Military organizations have employees and facilities distributed across long distances. Employees should be able to access shared data stores as securely and easily as if they were sitting at a desk in the home office. However, leased data lines are very expensive and of doubtful security for confidential information. Expenses are huge when connecting distributed offices across the world via this method. Ideally, the organization could use the Internet to securely connect their distributed networks and individual users at the cost of only the connection fee to a local Internet Service Provider (ISP), thus only paying for access to the Internet at a fraction of the cost of leased data lines. Virtual Private Network (VPN) technology enables organizations to leverage the Internet, allowing users and networks distributed across the world to securely access resources. VPNs are enabled through the use of specialized hardware, such as routers, and also network drivers that allow VPN access. The protocol for VPN is based on the IPSec standard. IPSec-compliant software and hardware need digital certificates from a trusted Certificate Server in order to securely extend organization networks to distributed offices and remote users.

9. Activities for implementing an organizational PKI

An *organizational public key infrastructure* is defined as a PKI that is used by an organization to support its own processes, which may be of a command, manage or business nature. We try to identify some important steps in the process of implementing such PKI.

Analysis of Operational Requirements PKI should be implemented to meet clearly defined operational objectives. The primary objective of this activity is to determine the processes that can be supported by the PKI, and the nature of those PKI services. It must also decide to implement a PKI in conjunction with the implementation of an application that will use PKI-based security services. If you do so, you should still consider the overall requirements of your organization to ensure that the PKI you are about to implement would meet more than the requirements of a single application.

Analysis of Certificate Policy Requirements It must define the quality of the PKI security services needed in order to support your operational processes. Quality is normally established by specifying certificate policies:

- Methods to identify and authenticate applicants who receive keys and certificates
- Obligations and liabilities to be expected of the subscribers, relying parties, and the certificate authority (CA)
- Procedures for a variety of topics, including certificate application and revocation, the collection of audit records, and records archival
- Technical aspects of key generation, delivery, and usage, cryptographic modules, activation data, and computer and network security
- Physical and procedural controls, which cover such topics as physical safeguards for the CA facility, specification of CA roles, and key changeover and recovery

- CA personnel security controls, including specifications for security qualifications, experience, and training
- Profile of certificates and certificate revocation lists.

Analysis of PKI Solutions There is a number of PKI solutions available on the market. You must review these products and identify those that can meet your requirements. Examples of things to consider are: maturity of the product, number and types of installations, users' level of satisfaction, conformance to standards (PKI, cryptography, communications, directory), product functionality, availability of integration toolkits and their ease of use, availability and quality of product training, vendor's product evolution philosophy and release strategy, etc. At the end of this activity, you should have an idea of the potential PKI solutions.

Analysis of Network Infrastructure The next step is to review your network infrastructure and identify the work required to integrate the potential solutions. You must analyse communications protocols, directory protocol, Internet connection for accessing PKI services from the Internet, entry points protected by a firewall, etc. Answers to such questions will provide you with information that will serve as input to the cost-benefit analysis.

Analysis of Cost-benefit: The analysis should clearly demonstrate the costs for your organization to implement, operate, and maintain its own PKI, versus the cost of purchasing PKI services from an established CA. You must select the PKI implementation option that best meet your organization's needs.

Integration of PKI Applications A PKI gives you the ability to use public key-based security services to support you operational functions. Before you can benefit from these services, however, you need to integrate the security service requests into your applications, or you must replace them by, or upgrade them to, applications with such requests already integrated. It is important to devise early a strategy for integrating PKI-based security services into your environment. Integrated applications should be introduced gradually into your environment, possibly starting with e-mail and other office automation applications.

Analysis of Policies and Standards This activity consists in reviewing policies and procedures that apply to your organization's activities, and all related security policies, standards, and procedures, for the purpose of understanding the framework under which the certificate policies are to be developed.

Development of Certificate Policies Results of the operational requirements analysis, the certificate policy requirements analysis, and the policies and standards review should provide you with the information you need to either adopt existing certificate policies, or to develop your own. Certificate policies contain specifications for security controls, CA practices, certificates, and keys, which must be implemented within the infrastructure. If you need to accept certificates issued by another CA, it might be wise to adopt policies that conform to, or to develop policies consistent with, the IETF's framework.

PKI Architecture The PKI architecture is typical system architecture. It should specify such things as hardware, software, and communications components, communications protocols, directory software and structure, cryptographic standards, and CA facility security.

Threat and Risk Assessment Organisations with established IT security risk management policies and standards may want to assess the suitability of their PKI architecture and the technical and administrative safeguards they are about to implement so as to determine the level of risk to their CA operations. Depending on the results of your threat and risk assessment, you may have to go back and modify the certificate policies and your PKI architecture so as to reduce the risk to an acceptable level.

PKI Design Your PKI's design depends on the certificate policies your CA will be supporting and the PKI solution you have selected. During this activity, you will describe in detail your PKI implementation, including the specification and configuration of network segments, and hardware and software components. You should prepare an itemized inventory of servers, workstations, routers, hubs, cables, network interface cards, firewalls, un-interruptible power supplies, and any other hardware and software components that you need to purchase. The PKI design document should also contain an inventory of changes to existing components.

CA Facility Design Based on your certificate policies, you must select and design a facility to house your CA's main components. Your design should cover construction requirements and the specification of physical and environmental safeguards. Deliverables from this activity should include an inventory of items to purchase and an inventory of changes to existing elements.

Personnel Selection The trustworthiness of your CA's operations will depend largely on the personnel you assign to the various roles. You need to select your PKI personnel with care according to the relevant stipulations of your certificate policies. Selecting your team at this stage will ensure their participation in the implementation activities, which provides an opportunity for knowledge transfer and learning.

CA Operations Manual The manuals typically supplied by vendors with their products rarely offers sufficient documentation, as they do not contain the operational procedures specific to your implementation. It is therefore recommended that you develop a manual containing detailed procedures covering all of the day-to-day operations. The manual should also cover maintenance and support.

Certification Practice Statement To support legal requirements, you probably have to prepare and publish a certification practice statement (CPS), which is a statement of the practices that your CA employs in issuing its certificates. The CPS describes the equipment,

the policies, and the procedures you have implemented to satisfy the specifications of your certificate policies. Like the certificate policies, your CPS should be consistent with the IETF PKIX Part 4. It will contain high-level statements from the PKI and CA design documents and the CA operations manual, as well as the general provisions expressed in the certificate policies.

PKI Implementation Plan As for any IT system, you should prepare a detailed implementation plan that covers activities for acquisition, installation, configuration, testing, certification, accreditation, and training. The plan should also contain a detailed schedule, complete with tasks, resources, and start and end dates.

Hardware and Software Acquisition Time to order your hardware and software components. You may wish to start this process as early as possible to avoid unnecessary delays.

Installation, Configuration, and Testing During this activity, you will construct the CA facility, and install and configure the hardware and software components as per your PKI design documents and your CPS.

PKI Training You should develop a training plan for your PKI personnel. Training should cover operations, maintenance, and support. Your PKI solution provider will probably have an adequate training program that can be tailored to include all of the procedures specific to your implementation. PKI personnel should also participate in the installation, configuration, and testing activities.

PKI Certification and Accreditation Certification of your PKI is equally important, a process by which you measure your PKI's actual implementation against its design. This type of certification may be conducted internally; however, having an independent and qualified firm conduct it for you will add credibility to the process and help establish the trustworthiness of your CA's practices.

Operations It may now begin to receive subscriber applications and issue certificates.

10. CONCLUSIONS

Internet is changing the way military activities are conducted. PKI is the enabling technology that simplifies the management and security of this process. With the right PKI implementation, military organizations can spend less time worrying about security, and more energy on their main activities. For example, confidential documents no longer need to wait for days to be physically shipped. Instead, they can be securely sent through e-mail. Web servers can allow secure access for only designated users, eliminating the need for human intervention. Military organization networks can securely extend over the Internet, eliminating expensive leased data lines. PKI's possibilities are limitless. For *Romanian Armed Forces*, the Public Key Infrastructure (PKI) capability may adopt the following components:

- Certificate Authorities,
- Local Registration Authorities,
- Certificate Directory,

and principles:

- use commercial products,
- use smartcards for protection of cryptography, digital signature, access control, keys and certificates.

REFERENCES

Burr W. E.. "*Public Key Infrastructure Technical Specification*", NIST, 1997.

DoD PKI Program Management Office, "*X.509 Certificate Policy for US DoD*", version 5.0, 1999.

DoD PKI Program Management Office, "*PKI Roadmap for DoD*", version 3.0, 1999.

Ford Warwick, Baum Michael, "*Secure Electronic Commerce – Building Infrastruture for Digital Signatues and Encryption*", Prentice Hall, 1997.

Gerk E., "*Overview of Certification Systems – X.509, CA, PGP and SKIP*", Meta-Certificate Group, 1998.

King, C., "*Building a Corporate PKI*", INFOSEC Engineering, 1999.

Marinier, F., "*25 Steps to the Implementation of a Corpoate PKI*", Labcal Technologies, 1999.

Patriciu,V.V., **Pietrosanu M., Bica I., Cristea C.**, "*Securitatea informatică în Unix şi Internet*", Ed Tehnica, Bucureşti,1998;

Patriciu,V.V., **Pietrosanu M., Bica I., Voicu N.**, **Vaduva C,** "*Securitatea comertului electronic*", Ed All, Bucureşti, 2000;

Patriciu,V.V.,"*Semnarea electronică a documentelor*", PC-Report, dec., 1998;

RSA Security S.A., "RSA Keon Certificate Server Product Overview", 1999.

Schneier B., "*Applied Crypography*", John Wiley & Sons, 1996.